# Avoid the Hidden Costs of AD FS with Okta

**Okta Inc.**
301 Brannan Street, Suite 300
San Francisco CA, 94107

info@okta.com
1-888-722-7871

wp-adfs-031413

# Table of Contents

# Challenges of Single-Sign On Deployments

As everyone knows, the adoption rate of cloud applications has been dramatic in recent years. Trials of applications like Salesforce.com, WebEx, or NetSuite have transitioned to enterprise-wide deployments, and many organizations have, as a result, either devised policies for cloud applications or are looking to do so in near future.

However cloud adoption is not without its challenges. The tendency of cloud applications to be silo'ed has made managing user access and authorization an increasing challenge. The task of onboarding users is a time-intensive, manual process that involves administrators across multiple departments, which can also introduce risk. For example, because there is frequently no central user directory, when an employee leaves an organization their access is often not revoked right away.

As a result, many enterprises today are looking to implement a single-sign on (SSO) solution that enables their users to easily access all of their cloud and web applications. A key requirement of these solutions is Active Directory integration, i.e. connecting all of their cloud applications back to a single source of truth, Active Directory.

Many companies conclude that Active Directory Federation Services (AD FS) is the best way to make AD integration happen. After all, both Active Directory and AD FS are from Microsoft, so that should be the best choice, right?

It's important to realize that not all Active Directory integration solutions are created equal, and IT departments should examine all aspects of implementation when considering AD FS for a SSO solution. One example is that AD FS is not exactly free. There are a number of hidden costs associated with it such as setup, ongoing support and hardware requirements. Secondly, if you're looking for a true SSO solution, AD FS is not it. AD FS does not provide features such as provisioning, mobile applications or reporting. In addition, integration is manual and does not support the 1,000s of applications that today's companies are using.

This whitepaper will discuss the hallmarks of a successful Active Directory integration and SSO deployment, and will compare Okta's 100% cloud based service to AD FS and its on-premises toolkit approach.

# Key Elements of a Successful SSO Solution

There are many items to consider when investigating SSO implementation options. It helps to focus on a few key elements to ensure success. While many of these checkboxes may not appear to be a major issue initially, over time as companies and applications scale, these items can become more frustrating for companies and end-users.

### Application Integrations and Support

The ability to support all of your applications, both today and in the future, should always be considered when looking at a company-wide solution. There may be one or two cloud applications to integrate today, but what is your company's longer-term strategy? In a recent survey, Gartner found over 70% of IT buyers in the United States and Europe and over 80% in Asia Pacific plan to increase their support for cloud applications by 2014[1].

As your applications scale, they may have different configuration requirements that may change over time, requiring an IT admin to stay on top of individual apps. The labor and setup associated with each application can become a drain on both employees and IT budgets.

### Availability

Any downtime associated with your SSO deployment means downtime for your users. This downtime may be planned, but it may also be unexpected. An SSO service and associated support must be agile to work with application configuration updates that may be altered by the provider. Ultimately any downtime means employees are not getting the access they require to do their job – lowering productivity for end-users.

### User and Access Management

Given a main value proposition for SSO is to support end-user productivity; user management should be inherently simple for the IT departments. The task of provisioning and deprovisioning applications for users should be simple and easily accomplished. In addition, a group-based management system should be implementable to allow for users to quickly gain access to the broad set of applications they may need. If an employee were to switch roles within in an organization, it should also be simple for the IT department to change their application access seamlessly.

### Logging and Reporting

Many regulatory agencies (e.g. SOX, HIPAA) require audit trails for users. This often includes seeing what employees have (or had) access to. If an employee were to leave a company, IT departments would be required to provide details around application access and de-provisioning. As usage increases by two factors, number of users and number of applications, aggregating this information becomes a difficult and daunting task. SSO solutions should be able to gather usage information for IT admins to quickly meet necessary company and industry reporting requirements.

### Active Directory Integration

Perhaps most importantly, an SSO solution must enable you to continue to use your existing user store (Active Directory), and keep all of your cloud applications synchronized with AD. The rest of this paper focuses on this critical requirement, and compares Okta to AD FS.

## Active Directory Federation Services as a SSO Solution

With the launch of Windows Server 2008 R2, Microsoft released Active Directory Federation Services (AD FS) 2.0, which is intended to provide a platform for handling single sign-on with cloud applications outside of the firewall. This ostensibly allows organizations to leverage AD FS to address the AD integration component of SSO, but can only be considered a reasonable solution for specific use cases.

When considering AD FS to address SSO needs, it's imperative to consider the platform. As a feature of Windows Server, AD FS was developed to be a toolkit—not an end-to-end solution for single sign-on needs. Toolkits can be flexible, but they require a significant amount of additional work to develop a complete solution. And that's work your IT team needs to perform.

AD FS is a “free” solution, so why wouldn’t all organizations use it? Several reasons: AD FS–based solutions require hardware and software (there are three server roles that make up AD FS itself: the Federation Service, the Federation Service Proxy, and the web server agent). AD FS also requires custom development and maintenance, and administrative time to understand, configure, and maintain the SSO connections with the target cloud applications. When you factor in all these requirements, it becomes clear that a solution based on AD FS is not actually free, nor is it scalable for a large number of applications.

To configure AD FS you must obtain a valid SSL certificate (self-signed is sufficient for testing, but third-party signed is necessary for production). Setup involves importing the SSL certificate, exporting certificates, and creating shared certificates to establish trust between your AD FS server and the target federation service. When trust is established, you must then generate the claims rules appropriate for authenticating with the target cloud application.

Claims rules can vary greatly based on the cloud application the system is integrating with. Administrators must know the Uniform Resource Identifier (URI) of the cloud application, which claims the application requires, the URL the application should expose to the user, and finally, whether the token should be encrypted. AD FS provides a flexible rule engine that can handle most situations, but you must not only define those rules for all integrations, but you must also continuously maintain them as the target cloud application changes.

Searching blog posts, websites, and technical documentation to discover the appropriate claims rules for each cloud application is time-consuming and unreliable. The rules for each application may also change over time, invalidating your SSO integration, so tracking those changes is necessary.

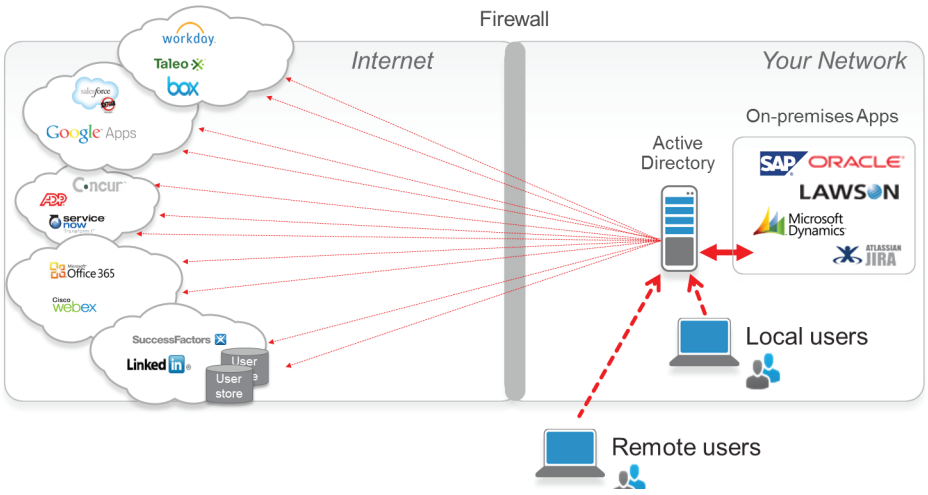


*Figure 1: AD FS requires integration for each individual cloud application, which is difficult and costly to maintain.*

Once you establish the AD FS infrastructure and develop the appropriate claims rules for each target cloud application, it's still necessary to determine how users will actually use SSO to access these applications. Most likely you will have to either create a portal where users can access these applications, or integrate access to them into the existing corporate portal.

Additionally, there are significant hardware costs associated with deploying AD FS. Microsoft requires a minimum of two servers to get up and running, a AD FS 2.0 server and an AD FS 2.0 Proxy Server. However, they recommend additional servers for high availability, which increases the server count to at least four. If you wanted to connect a service like Office365 via AD FS, a DirSync server is also required, upping the count to five servers – just to get up and running[2]! On top of that, there are space considerations and utility and maintenance costs. Those last three costs don't go away in year two.

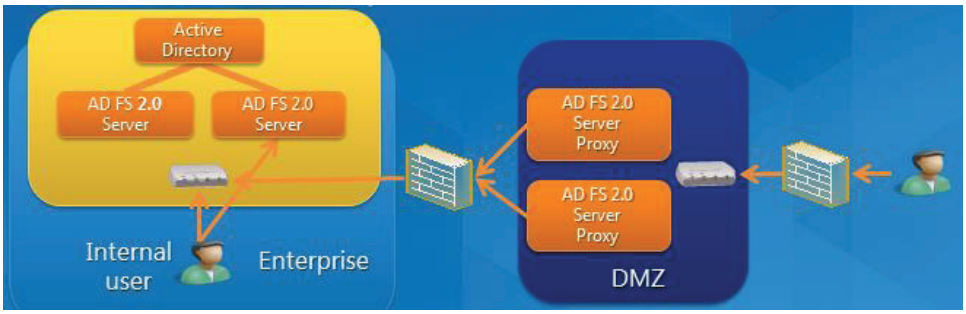


*Figure 2: AD FS architecture requires a minimum of two servers within the DMZ.*

Clearly AD FS is a powerful platform that can be leveraged to integrate AD with cloud applications. However, an organization must commit considerable time and money to achieve and maintain an end-to-end solution for all of their applications. Even then, AD FS only addresses one-third of Active Directory integration challenges.

Finally, AD FS does nothing to address one of the biggest shifts to happen in computing and IT in several decades: the shift to mobile computing. Any SSO solution you consider must address mobility for your end-users.

## Okta: SSO for All Your Cloud, Web and Mobile Applications

Okta is an on-demand identity management service designed to help companies accelerate the adoption of cloud applications across the enterprise. At the center of Okta's on-demand offering is the industry's most unified, comprehensive, and single-sign on solution.

The Okta service provides:

- A complete end-to-end solution that requires no services to install and includes:
  - Self-configurable, secure integration with your existing AD infrastructure.
  - A large catalog of pre-integrated business and personal applications.
  - A single sign-on home page for every user that offers one-click access to all of their cloud applications.
  - An integrated administrative experience that allows you to manage users, applications, and your AD integration from one console, anywhere, anytime, and on multiple devices.

- A 100 percent on-demand offering. Okta's core service is a multi-tenant solution with an AD agent that installs locally but without any appliances or servers to buy or maintain.

- Application integrations that are maintained for you. Okta manages and updates the integrations so you never have to worry about continued seamless integration as underlying applications change.

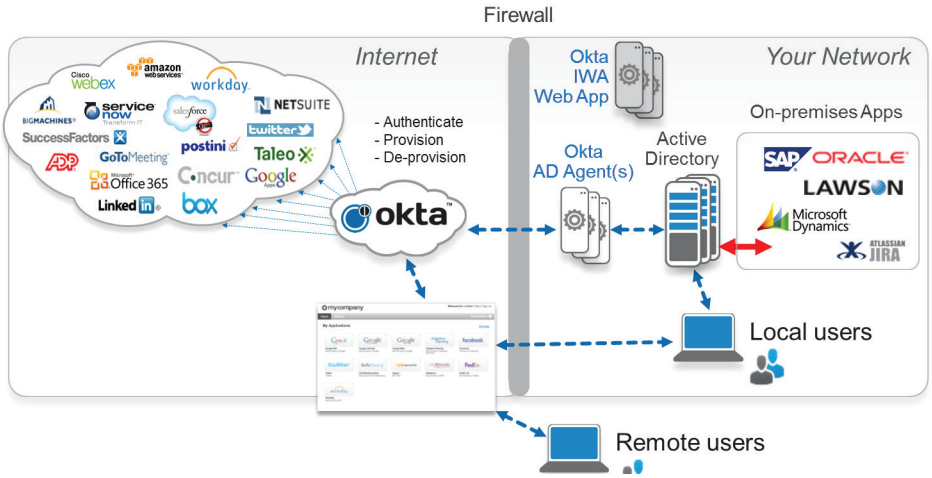


*Figure 3: Okta enables one integration point for all your current and future cloud applications.*

- Outbound AD connection over HTTPS. Okta's lightweight agent makes a secure, outbound-only connection over HTTPS—no firewall configuration changes are required.

- Out-of-band authentication. Okta authenticates a user with the cloud application and then gets out of the way. All ongoing traffic is between the user and the application.

## The Hidden Costs of AD FS

While AD FS is marketed as a 'free platform," in practice, it is rarely free. In order to fully implement AD FS, IT departments must spend their time installing and configuring cloud applications. While this may not seem like a large up-front cost, the number of man-hours required for each new application does not decrease with economies of scale. So if your company plans to scale from one application today to five or six in the next three years, it means your IT department will be configuring each new application. In addition, all the manually configured applications via AD FS require regular maintenance to ensure connectivity remains intact with corporate networks and infrastructure.

Okta reduces installation and maintenance costs and downtime risks by maintaining the relationship with cloud applications. Corporations need only to configure their networks with Okta once and we do the rest. Okta continuously manages and monitors cloud application integration to ensure you don't lose connection. In addition, Okta was developed with our customers in mind and is able to provide new updates to the product regularly with zero downtime – so you're always providing business critical application access to employees.

Okta is also able to provide a central portal of applications to your end-users. This enables them to easily access the applications that have been provisioned to them. A similar solution via AD FS would either need to be manually created in-house or outsourced to another company – further increasing company costs. So you could choose the 'free' AD FS solution or you could choose Okta and reduce your costs and while gaining additional functionality beyond basic SSO.

Let's look at it another way. If you have one cloud application to integrate with AD FS, the costs don't appear to be massive.

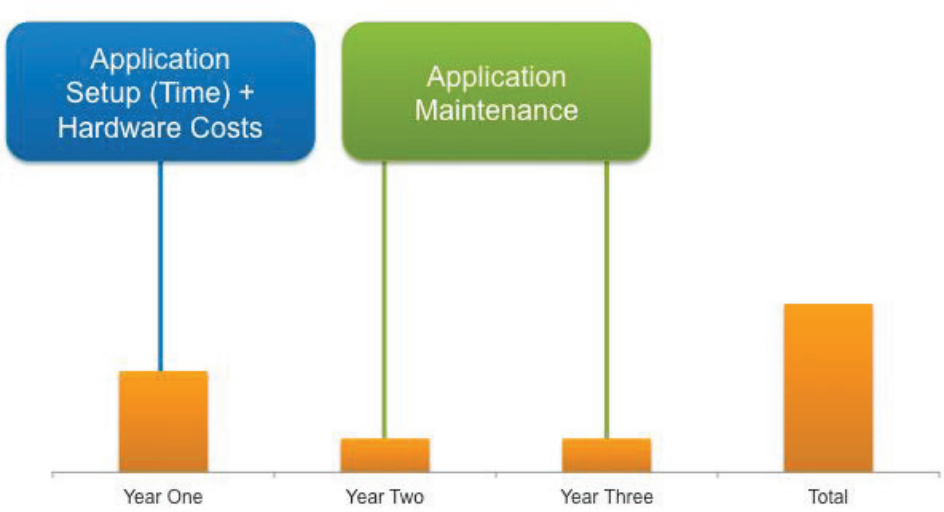


*Figure 4: Relative AD FS costs for one application integration.*

However, let's say you plan to add additional applications in the future. Adding a new application via AD FS requires the same level of configuration, installation and maintenance as the original application. This additional work and costs can add up for IT departments, especially as companies adopt more and more cloud applications.

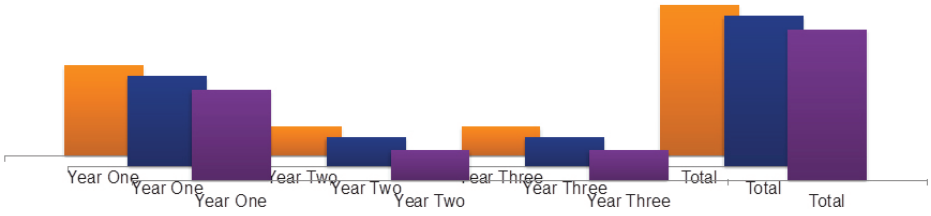


*Figure 5: AD FS costs can add up for integrating multiple applications.*

If you were to compare the three-year costs of AD FS to Okta, you would see be able to see that with each additional application, costs to the company remain constant. Okta does all of the integration work; so little effort is required by IT departments to configure new cloud applications to end-users. The cost for Okta never increases with new applications; therefore corporations will see larger savings as they continue to add cloud applications to their infrastructure.

## Okta versus AD FS Quick View Comparison

| Metric | Okta Approach | AD FS Approach |
|---|---|---|
| Application Integrations | • 1,000's of pre-integrated applications<br>• No need to configure and maintain application integrations<br>• SSO with any application, not just SAML or WS-Fed apps | • IT Admins build and maintain each integration<br>• Only supports SAML, WS-* |
| Availability | • 100% multi-tenant solution<br>• Always-on with zero downtime<br>• No changes required to AD infrastructure | • Must configure, install and manage<br>• Required maintenance as applications evolve<br>• Availability redundancy<br>• Requires multiple servers (installation & failover) |
| Access & User Management | • Control access to all your applications<br>• Easily map different username formats<br>• Easily add, change or remove users and access<br>• Import directly from AD, security groups<br>• Automatically configured for all integrated applications | • Must create and manage custom AD attributes<br>• Every application may require changes<br>• No concept of user importing, matching |
| Reporting | • Dashboard of metrics to see overall health of users and applications<br>• Easy access to user reports for compliance purposes | • N/A |

## Getting Started with Your Free Trial

To discover how easy it is to deploy Okta and to begin securely scaling your cloud-based applications, visit www. okta.com/freetrial to get started today.

1. *Gartner Research, October 2012.*
2. *Microsoft, September 2011. http://blogs.technet.com/b educloud/archive/2011/09/23/ questions-about-single-sign-on-sso-with-office-365-for-education.aspx*

**About Okta**

Okta is an enterprise grade identity management service, built from the ground up in the cloud and delivered with an unwavering focus on customer success. With Okta, IT can manage access across any application, person or device. Whether the people are employees, partners or customers or the applications are in the cloud, on-premises or on a mobile device, Okta helps IT become more secure, make people more productive, and maintain compliance.

The Okta service provides directory services, single sign-on, strong authentication, provisioning, workflow, and built in reporting. It runs in the cloud on a secure, reliable, extensively audited platform and integrates deeply with on premises applications, directories, and identity management systems.

Enterprises using Okta today include Activision, Allergan, BMC Software, Groupon, Informatica, LinkedIn, Purolator and SAP. The hundreds of enterprises, thousands of cloud application vendors and millions of people using Okta's identity management service form the foundation for the industry's fastest growing, vendor neutral Enterprise Identity Network. Okta's Enterprise Identity Network seamlessly and securely connects organizations, applications, and people, anywhere, anytime, from any device.

The Okta team has built and deployed many of the world's leading on-demand and enterprise software solutions from companies including Salesforce.com, PeopleSoft, Microsoft, BMC, Arcsight, Sun, and HP. Okta is backed by premiere venture investors Andreessen Horowitz, Greylock Partners, Khosla Ventures and Sequoia Capital.

For more information, visit us at www.okta.com or follow us on www.okta.com/blog.